The Future of Cybersecurity with Jeff Hall

CyberAware Podcast: Season 2, Episode 7

Nathan: Welcome back everybody. This week's episode, all things future of cybersecurity. My name's Nathan Sloneker, your resident expert on all things cybersecurity. And again, I'm here joined with Ham.

Ham: Dude, it is so great to be back in the studio once again, as always. As Nathan said, I'm Noah "Ham" Adamson and it's great to be on the mic always. Today, we have an extended episode featuring a special guest. In this episode, Nathan sits down with industry expert Jeff Hall to chat with the features of cybersecurity.

Nathan: Yeah, that about sums it up. Future cybersecurity, what technology is going to look like, what the jobs fields are going to look like in the future. And just a bunch of the unknown factors, you know, we're trying to wrap your head around and gauge what's going to be happening in the coming years.

Ham: Right, and even though just being a random dude off the street, like, it's so crazy to think about what this industry really has to offer, especially in the world of cybersecurity.

Nathan: Yeah. I mean, we covered a lot of great topics this episode. Some of my favorites included AI and machine learning.

Ham: Oh, nice. I love AI.

Nathan: It's not just cybersecurity, but technology in general. Fun episode today.

Ham: Oh, that's sick, you know, I'm super excited.

Nathan: All right, then let's get into it.

Hey everybody. Welcome back to the CyberAware Podcast. Season two. Uh, today I'm joined by Jeff Hall.

Today we're going to be talking about the future of cybersecurity. Brief introduction, Jeff, if you just want to talk about yourself here for a bit, who you are, what you're about? Things like that.

Jeff Hall: Sure. I'm Jeff Hall. I'm a principal security consultant with Truvantis based out in beautiful Silicon Valley, although I'm not there. What, what do I do? I do information security work. Currently I'm working as a virtual chief information security officer for a large software developer. We're dealing with all their compliance issues for ISO compliance, which is an international standard.

Nathan: Just a quick follow-up here, if you just want to briefly explain what compliance means?

Jeff Hall: Compliance is an interesting thing because it leads into a lot of arguments, but basically you're given a framework that says, do you do a, and you have to prove that, yes, you, you do do a. Whether that's, you know, for people, checking someone's driver's license to make sure that it's valid, that it's issued by a proper state authority that it's enforced at the moment. You know, it hasn't expired. That's an act of compliance.

Nathan: Okay. Yeah. I just thought that'd be good for the listeners to know. Cause I feel like that's a hot thing that we're going to be talking about a bit today. So I just wanted them to get a bit of an insight into what we we're talking about with it.

Jeff Hall: Sure.

Nathan: How long have you been doing security? How long would you say you've been in the field?

Jeff Hall: I started really doing information security about 20 years ago.

Nathan: Okay.

Jeff Hall: As a true vocation, I started in information security practice at a large consultancy. They kind of sorta had something, but it wasn't codified. It wasn't organized. And so I moved from management consulting, into information security.

Nathan: Okay. 20 plus years in the career now, I mean, for where we're at, technology-wise now versus back in the day, how far have we come would you say?

Jeff Hall: Well, it's an entirely different thing. I was doing information security prior to that off and on. I started out doing information security on mainframes, and then that migrated to what we now call the local area network, which involve Novell, NetWare, and ultimately brought Windows NT into the picture. And then the real explosion was in '95, when the internet hit the scene, it had been around for a long time as a protocol, a networking protocol. But, you know, we actually got what we have today, which is wide connectivity. And from there it's just been downhill.

But you know, prior to that, security was easy because it was all very, very sheltered, proprietary protocols. The mainframe had its own and they even had them amongst various vendors and they didn't connect well. And then NetWare rolled around and it had its own protocol. And we had to make that work within our own proprietary protocols, which typically involved hardware.

Nathan: Okay.

Jeff Hall: And then once everyone got an IP stack, which is the basis of how the internet works, then we started interconnecting stuff internally and then lo and behold, the internet rolled out.

Nathan: And the scale just increased tenfold. Unbelievably it just, yeah, it blew up.

Jeff Hall: I mean, I remember when I got my first true internet connection at home, I was on DSL over, uh, I think it was 56 KB. And then I upgraded to ISDN, which was a whopping 128 KB. And then broadband came into our area through the cable company. And the cable company, I was testing it for them. I was a beta tester for the internet for them in 1996.

Nathan: They hooked you up with the full package sort of thing then?

Jeff Hall: Oh yeah!

Nathan: That's pretty fun.

Jeff Hall: And so I had 10 megabit access. My kids loved it.

Nathan: We've come a long way since then.

Jeff Hall: Yeah. I'm running half gigabit now.

Nathan: It's just funny just hearing about the speeds from back then to how, what we're at nowadays. What made you want to get into security or just information security in general?

Jeff Hall: Well, it wasn't so much that I wanted to, it just ended up that way. I started out as, as a systems programmer on a computer system called a mainframe, which was what we had back when I was in college. I'm actually probably one of the few information security people that has a degree in computer science. Most people either got into it like I did, they started out in another area of the business and kind of fell into it. It's interesting. Very few people actually necessarily started out in IT and got into security.

Nathan: I, myself am going for computer information technology, but I do want cybersecurity when I'm out of college. So it is kind of funny. But you were saying that you, you think a decent amount of people actually start off different areas and then eventually find their way into security. Is that just general IT jobs or one more than the other? What do you think?

Jeff Hall: Oh, I mean, a lot of people that start out in programming, interestingly enough, have degrees in music.

Nathan: Music?

Jeff Hall: Yeah

Nathan: I never have heard that. Why would that be?

Jeff Hall: Well it's because music has patterns, notes, repetition, and a lot of musicians naturally gravitate to programming.

Nathan: Now that you mention that I can definitely, I could definitely see how those two would connect in that sort of way.

Jeff Hall: Yeah. I've, I've worked with a lot of people that either majored in music, minored in music, and just ended up going then into IT, because they found it helped their musical interests. It's an odd one, but yeah, it's an interesting, just an interesting connection.

Nathan: No, I agree. I personally, I never knew about that. So that's really interesting to hear about. You have a lot of knowledge in a lot of different fields. You know, with the security field in general, how focused can you get with just potential jobs and everything?

Jeff Hall: There used to be a saying that the higher you go in technology management, the further back in generations of technology you go. That's not so true today. What you find more and more is if you want to get into management, you're going to need not only the technology background, but you're going to need a business degree, whether that's an MBA.

The thing I liked being in the school of business where I got my degree is I was required to get a background in accounting, marketing sales management, as well as focusing on computer science, because I also got not only the usual, here's how you do programming. Here's how you manage projects. But I had electives and compiler theory and data. Well, at that time, it was called data analysis, which resulted in what became database design and those kinds of things. So my background is across not only technology, but general business.

Nathan: I've heard from multiple people that cybersecurity that's one of the best degrees you can get in is most people don't realize how much the business side ties into cybersecurity.

Jeff Hall: Without the business buy-in you don't have security. That's just the way it works. You have to get the business because it doesn't fall entirely on IT to secure things. We're required in it to make sure that there are firewalls and all this other stuff that's in there. But business has to control who has access to the systems. Why do they have that access? What can they do when they access? Can they only read the data? Can they update the data? Are they the source of the information? And all that comes with certain responsibilities that IT can't control. That has to be controlled by the owner of the application. And that owner is not in IT, that owner is in the accounting department, the marketing department, the manufacturing department, wherever. They all have responsibility.

Nathan: For overall, what kind of skills do you think security people will need in the future? Or, you know, what kind of minors would most people not consider useful for infosec field or cybersecurity field, but kind of actually are more useful than others?

Jeff Hall: We opened this up talking about musicians. I've run across people with marketing degrees that are security people, I've run across people that were salespeople and went into security. It just depends if you have the interest. A lot of those people succeed because they have a degree that is outside of the IT business so that they can then relate to and communicate with the business people. Because the true security people that are doing firewall management, for example, that are dealing with the network, that are dealing with the technological, the very techie aspects of it.

They're the ones that have the problems communicating with the rest of the world. That's why it's best to have this focus on the business world, as well as IT. And even if you don't have the IT aspect, the deep IT aspect, as long as you have an appreciation for the IT aspect, you can succeed in information security.

Nathan: Okay.

Jeff Hall: You know, project managements skills are, are well needed in infosec.

Nathan: Oh, I can agree with that. As long as you have the, like the, the want to be in IT, you can succeed as you're saying. And going back to the minors, I personally, I'm going for computer information technology and my minor is criminal justice. I have friends who are also CIT and their minor is automotive technology. You had talked to Mercy when we originally met and she has graphic design. It's crazy just how broad you can get with information technology in general and at the same time with your minor, how that can tie into what you want to go into.

Jeff Hall: And you bring up the criminal aspect. That is a growing field as well. Local law enforcement and from there on up, whether it's local county, state, federal. They're crying for technology people that understand not only the security aspects, but then how do you investigate these crimes that occur? One of the topics we had that we wanted to talk about was, does technology, new technology imply new crimes? And really not. We're just seeing the criminal aspect move into the technology space and leverage it to facilitate whatever they want to do, whether it's a Ponzi scheme, you know, the traditional fraud that would have been done through the mail or over the telephone is now being done over instant messaging or texting. But it's the same stuff, just using a different platform. And sadly law enforcement is just totally behind the eight ball because they just don't have the arms and legs to deal with it.

Nathan: That's one of the reasons I am going for what I'm going for right now. Is there a shortage of people for infosec and cybersecurity jobs?

Jeff Hall: For forensic work, yes, there is truly a shortage because as you're well aware through your schooling, there are rules of law you have to follow when you do forensic work. And if you don't do it, it's inadmissable in court and lawsuits can happen.

Nathan: The fine line to walk.

Jeff Hall: Right. In that regard, there is a shortage, but in regards to information security people as a whole, the problem, there was an article published, a study done by Accenture and someone else that basically said the whole problem with not only the information security shortage, but hiring shortages in general, is being now tied to their applicant tracking systems. They have become so reliant on their ATS systems that they can't get the people through them so they can interview them.

Nathan: Do you want to explain quick what ATS means?

Jeff Hall: So an applicant tracking system for anybody that's applied for a job these days, particularly if you're online, whether it's through Monster or the company's website that does it, which is typically outsourced to a third party that runs this applicant tracking system. When you put in your resume and it reformats it, it's running through a series of algorithms, looking for key words and whatever else that the HR person or the recruiter was told to look for. And then that system grades your resume. And if you're above a certain score, say, there's a one to a hundred scoring system. If you're above a score of 60 or 65 or 70, whatever it may be set at, then you get picked out, right? You get kicked out as a potential candidate. And so what you end up having is, is people play all sorts of games to get past the ATS.

Nathan: The one that I'm aware of is putting words at the bottom. If you can find the keywords and making it white, white text, I've heard that one.

Jeff Hall: Yeah. Yeah. There's that one. There's hashtags. There's all sorts of stuff. In sadly, I had a company who really, really, really, really wanted to hire me and I couldn't get my resume through their ATS system. We even tweaked my resume to hit all the high points in their ATS system. Couldn't make it happen. And after about two months of screwing around with this thing, we all gave up and walked away. So this is the problem. A lot of the people shortage is HR and the hiring managers are not properly configuring things to get people through the door. We know this is going on because people now are posting out on Twitter and LinkedIn all the stuff that fails, you know, like, oh, I want an entry level person with 10 years of experience in the following. Pardon me? My favorite one was the guy who invented Kubernetes. It was a large corporation and a technology corporation, nonetheless, who was looking for people with 10 years of Kubernetes experience. And it's only been in existence for five.

Nathan: Yep. I remember hearing about that. Even entry-level jobs, in some cases aren't entry level anymore.

Jeff Hall: Also the hiring managers are looking for unicorns. You know, I want somebody who has five years of experience with Slack and has 10 years of experience and in Java. And, and it's very, very, very, very specific down to skillsets and experience and there's nobody running around that's going to fit that. And because of the ATS, nobody who could maybe hit 50% of it –

Nathan: Would even get through?

Jeff Hall: Well, and this is why networks are everything. This is why LinkedIn and connecting with people like myself, yourself, whomever, and building and working a network is so important. I just changed jobs in August. And the reason that occurred was I had someone in my network. They really, really wanted to hire me. "Would you change positions?" And it was out of the blue.

You know, the old thing used to be, "it's not what you know, it's who you know." Today's derivation of that is, "it's what you know and who you know," because if you're an expert in a particular field, stay forensics, and you have a good network, you'll never be out of work.

Nathan: Networking is the whole game. Nowadays. College students, especially in IT, like networking is one of the biggest things that you can start. I started networking recently and Dr. V introduced me to you, you know, networking like that. And here we are. It's things like that, but networking is just so important nowadays, especially for this field.

Jeff Hall: And the key is not to treat LinkedIn like Twitter or Facebook, cause people get turned off in a heartbeat. LinkedIn truly does try to be more business focused and-

Nathan: Professional.

Jeff Hall: Right. What you want to do is get connected with people. You want to read what they post because people like myself, I'm posting stuff that I think is going to be helpful to people, whether it's the latest exploit or an article from Harvard Business Review, whatever. I'm just trying to help people think outside of the box, little bit broader, keep abreast of what's going on in the world. I've been posting a lot of stuff lately about work from home because that's been a huge bugaboo in information security circles, because how do I secure somebody when they're at their house?

Nathan: You don't know who's doing what, when, where, whatever. That's their own, you can't, you can't govern that at all.

Jeff Hall: They're on their wifi and everybody knows mom and dad's wifi password.

Kids could be doing whatever as well.

They're in school and doing God knows what and you know, when the pandemic hit, there was a lot of us that scrambled to give people advice on how to secure people that were now going to work from home, Starbucks, wherever.

Nathan: It's just changed workflow so much, especially in our field as we are information security. We work on computers, you can work remotely. And I feel like a lot of companies and people are seeing that, oh, wow. This might actually be what we should move into. I don't have to pay my heating. If you're not coming into the office, I don't have to pay for your wifi. You don't have to spend gas to drive here.

Jeff Hall: An office based in a downtown location's not cheap, so if I can keep people working out of their home and only have to have 10% of the office space I need, hey, all I'm all for it. Major consultancies have, have found this as a boon. I haven't had an office since almost 10 years. I've been working out of my home office since 2013. I had an office. Was I always in it? I was in the office usually Tuesdays through Thursdays. I was not in on Mondays or Fridays. And because I've been a consultant most of my life, you're out at a client's workplace. You're not in the office. They don't want to see in the office really.

Nathan: At the end of the day, for some people it's more efficient than actually having everybody come in. The company overall is going to be saving so much more money and I'm sure the people are happier not having to spend theirs to come to work and whatnot, if you just say work from home, you know?

Jeff Hall: Yeah. But when it comes down to that, it becomes a trick because how do you make sure that's secure? There was an article I was kind of laughing about this week about a company that has created spyware for business whereby it monitors your camera every minute. And if you're not there, alerts your boss that you're not in front of the camera.

Nathan: That's weird.

Jeff Hall: The person who wrote the article was explaining that all of this office place protocol goes back to World War II. It was found in World War I that people were more productive when they were grouped together and managed properly. And now we're seeing the pendulum go back to, well, maybe we don't need everybody to be around all the time, which interestingly enough, if you go to Japan, that's exactly how Japan sorta operates in a lot of ways.

There are a lot of businesses in Japan that are in the first level of a family's home and they live above it. Yes, they have tall skyscrapers and whatnot. But a lot of the work is actually done in people's homes.

Nathan: Japan is cutting edge for technologies in society, hands down. That leads into one of the things that we want to talk about, AI and ML. For anyone who is listening, that's artificial intelligence and machine learning. Japan has become so automated. I read something like a year ago about they had teacher robots now that are teaching everything. For you, what do you think that's going to mean in the future? If ML and AI, if that becomes like complete automation in security?

Jeff Hall: I would like to tell you that it will be completely automated, but probably not in our lifetimes.

Nathan: I think when we discussed it, you said it's something that everyone has been talking about every year for 20 years.

Jeff Hall: I remember in the early eighties, AI was just around the corner. It was just a matter of time. Once PCs came outand whatnot. Oh, it was, "by the end of the decade," blah-blah-blah and here we are 40 years later.

Nathan: By the end of the decade.

Jeff Hall: Yeah, it's better. And yeah, we're doing things better, but it's still sketchy. The thing people should know, AI really is nothing more than an if/then table. If this, then do this, if it's not that, then do this. If it's not that, and you just keep going through and becomes a longer and longer and longer list.

Nathan: Yeah.

Jeff Hall: It's not anything magical. What is magical is machine learning . It is a very interesting field. I had a friend who went to MIT that, that got into it in the late eighties. Just fascinating the algorithms and how stuff works and how they learn, uh, if you want to see a

learning machine you can look them up on YouTube, the dancing robots and all that stuff. That's amazing.

Nathan: There's YouTube videos that I've watched that are so interesting to watch. People will make kind of these games, okay. I remember there was a hide and seek one where they had like two hiders and two seekers and they had a little arena. And the goal obviously for the hiders is not get found, goals for the seekers is to find the hiders. And as the machine just started learning, they started breaking the game. And it's so funny because they got to the point where they got so efficient. They started glitching out of the map that was created for them. And this was just, just letting the machine run. That's it. ML is just so crazy how in depth they can get and how smart machines can be just from learning.

Jeff Hall: In some ways AI and ML are going to take up mundane tasks. There's no doubt about that. Whether it's information security, making your hamburger. I mean, I worked with a robotics company back in the late nineties that had robots that flipped burgers and ran the fry machine. And when the pandemic rolled out, their sales went through the roof because no people in the restaurant, or fewer. Robotics and AI and ML have been around. But are they going to replace people? Yes and no. Yeah, there's, going to be some jobs that get eliminated, but by the same token, there are going to be jobs created because they need to be maintained. They need to learn. Not only that, but, the big thing in machine learning right now is how do we stop machine learning devices from learning bad habits? The latest thing is to hack ML by feeding it bad data.

Nathan: When it comes to machine learning, there are some scary things I can come with it. The whole Skynet is going to take over sort of thing from Terminator. I mean, there are potential vulnerabilities. And it just comes down to making sure that all that sort of thing is secure. But when we're playing with something like this or creating stuff like this, there's so many unknown factors at the same time.

Jeff Hall: All you have to do is look at the latest investigations into the Tesla racks and department vehicles. That is an AI, ML situation whereby what did the ML learn? Or what isn't it learning, because why are these cars driving into parked vehicles?

Nathan: You know, people always are talking about possible vulnerabilities. Tesla would pay hackers to come in and hack their car. And it was surprising how many you were actually able to.

Jeff Hall: Any modern car that has access via over the air, which most do nowadays? They can all be hacked.

Nathan: And we're not talking like Tesla with the self driving in that sort of sense. I mean, cars have all sorts of different things.

Jeff Hall: Cadillac has their version and Ford has their version. I remember attending, uh, the Consumer Electronics Show back in 2002 and I was in and, uh, presentation for audio systems in automobiles. And there was a guy talking about, oh, "here's the brave new world for your car. Your music, you won't have CDs anymore. It'll all be digital and you'll pull into your garage and it'll automatically sync with your Hi-Fi at home." And, okay, great. So the Q

and A comes at the end and I asked, what are you going to do to stop the guy from hacking the audio system in my car? And, lot of puzzled looks on the panel. And one of the guys from one of the other companies said, why would anybody do that? And I said, well, why would anybody want to get my tax returns off my home PC? They do it because they can. And what are you going to do to protect my car from somebody stealing my music, putting something in the car that shouldn't be there. At that point, the concept of a car network was just evolving within the automotive engineering industry. And they were coming up with these new standards. It was scaring those of us in the technology business because they weren't discussing security

Nathan: They were doing all these cool inventions and stuff, but security was at the back of their minds.

Jeff Hall: Most people don't realize that every automobile has a black box inside it now. So when you're in an accident, they can pull that module out and they can download. When did you hit the brake? How fast were you going? What was the temperature? Was the engine overheating? Was, you know, whatever, all that stuff, just like they can with an airplane, they can get a data recording of everything that was going on, including location.

Nathan: One thing that I did really want to discuss with you during this, as we are kind of running out of time here is, cyber warfare. I don't know what your opinion is on that. Like how people are saying, we're kind of in a new age Cold War with everything going on in the world. I mean, there's countries that are hiring people to just come hack for them.

Jeff Hall: We do it all the time. The UK does it. I mean, what was it last year? The Israelis had to admit that they had hacked us.

Nathan: I'm well aware of the U.S. Would as well. You know? No one's hands are clean in this sort of sense.

Jeff Hall: I mean, is it a new age Cold War? Kind of in a sense in that you have China, Russia, other non Western entities, let's call them that, going after Western entities, but it's not even that. Although, that seems to be what everybody focuses on. I can tell you because of work I've done with companies, it's also your friends, your business partners, anyone that you allow internal access on your network is likely filching data in one way, shape, or form. So it's a Cold War in the sense that the government is worried about the old fashioned Cold War, government style actors, but cyber warfare is a daily thing. It's not limited to where, oh, it's just Vietnam or it's Afghanistan or if it's Iraq. No, no, no. This is going on every day, every hour, every minute. People are trying to do digital attacks and trying to see what they can gain access to. And therefore, how do we get the information that we want? Some of it is espionage. Some of it is just people with nothing better to do. Ransomware is the obvious thing. We encrypt an entity's files and tell them we'll give them a key to get it back. But is it a new age Cold War? In a way it is, but in more ways than not, it is not.

Nathan: Fair enough. We're running about an hour now, so I don't know about you, but I think we're at a good place to call it. We covered more than what we had originally. So I'm happy with that. Thank you for joining us today. I learned a lot personally, so I appreciate you coming in and just sitting down and talk with us.

Jeff Hall: Great to be asked and great to be here.

Nathan: At the end of episodes, we like talking about our takeaways. Um, I really think machine learning is a fun thing to look into for anybody. It's so fun to learn about and watch and just see. AI and ML are both super interesting to me. How about you?

Jeff Hall: For me, if you're going to take away anything from this, keep all your devices current and up-to-date. So don't, don't delay updating your iPhone. Don't delay updating your iPad, your Android device, your tablet, your PC. When patch Tuesday rolls around, second Tuesday of every month, update your Windows device. All you Mac users out there, you're just as susceptible as everybody else. So don't believe all the hype that Apple pumps out there. Yes, they do a very nice job trying to protect you, but it's not perfect. If you learned anything from today's discussion, keep your devices current.

Nathan: Agreed. And for anyone who wants some more information on that, we did cover that in our first episode. Just ways you can stay safe. So going off of what Jeff said, definitely. I agree with him a hundred percent on that front. Thank you again, Jeff, for joining us today. I really appreciate you coming on to talk with us.

Jeff Hall: Glad to be here and glad to share my experience and knowledge.

Nathan: All right. Well, I guess now we'll just pass it off to Mercy for the news.

Mercy: Hey everyone. Mercy Ayesiza here with the news, a student expert on the information security team. I'll be updating you with what's going on in the cybersecurity world. Before I get into the headlines, please make sure to subscribe to our podcast and today's highlights are –

A major cyber attack hits Robinhood, affecting 7 million users. On November 3rd, 2021, Robinhood, a financial service and stock trading company, was hit with a cyber attack that ended in 7 million users' personal information exposed to the cybercriminals. Personal information gained in the breach includes names, email addresses, and for some users, information like date of birth and zip code. The cyber criminal, whose name has not been disclosed yet, gained access to the customer support systems through social engineering. They called the customer support agent and lured them into disclosing information about the customer support system.

Our second news update today, a phishing campaign mimicking cybersecurity company targets Microsoft 365 and Google users. Proofpoint, a cyber security company, was imitated by a cyber criminal who was digging for Microsoft 365 and Google email credentials in a phishing campaign that was able to bypass Microsoft email security.

That email is said to have included a mortgage related file sent via Proofpoint, with a confidentiality notice at the bottom. According to the researchers at Armorblox, an email security company, clicking on the link redirected the users to a fake website that looks similar to Proofpoint, which then asks for Microsoft and Google email login credentials. Remember

to practice cyber-hygiene with your passwords along with multifactor authentication across all your accounts and be cautious of such phishing attempts by investigating before clicking.

Our third and last news update today is – Mozilla Firefox now available in the Microsoft Windows Store. Firefox, a well-known browser, is now included in the Microsoft Store for Windows 10 and Windows 11 users as of November 9th, 2021. Before, users had to go to the internet to download and run the Firefox installer. Now, you can download Firefox quickly and easily from the Microsoft Store on your device.

And that wraps up the news for this week. Thanks for listening to the CyberAware Podcast we'll see you next time.